US Department of the Treasury
Financial Management Service
Financial Operations
Financial Processing Division
Treasury Check Information System (TCIS)
Privacy Impact Assessment (PIA)

Name of System: TCIS
Bureau: Financial Management Service
Financial Operations
Financial Processing Division

A. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals? Yes

a. Is this information identifiable to the individual[1]? Yes
(If there is NO information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the PIA does not have to be completed.)

b. Is the information about individual members of the public? Yes
(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security Certification and Accreditation (C&A) documentation).

c. Is the information about employees? No
- Employees only included as members of the public
(If YES and there is no information about members of the public, the PIA is required for the FMS IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

2) What is the purpose of the system/application?

TCIS is a "TIER II" mission supportive application system that is designed to support the FMS Financial Processing Division. TCIS will be used in recording and reconciling the worldwide issuance and payment of U.S. Treasury checks.

[1] "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

This system will also query Payments, Claims & Enhanced Reconciliation (PACER) for Automated Clearing House (ACH) payments.

3) What legal authority authorizes the purchase or development of this system/application?

Various statutes authorize FMS to carry out its core functions of issuing and reconciling Treasury checks. TCIS is a system that is necessary to accomplish these functions and is therefore authorized by the same statutes. They are: 31 USC sections 321, 3301, 3327, 3328 and 3334.

B. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

Any payee associated with receiving a Treasury check or ACH payment.

2) What are the sources of the information in the system?

TCIS sources are listed below:

Sources of Daily Inputs:
* Non-Treasury Disbursing Offices (NTDOs) send check issue information.
* FMS Regional Financial Centers (RFCs - 4) and FMS Debt Management Center (DMC – 1) send check issue information for payment requests received from FPAs.
* FMS POL system sends Available Check Cancellation (ACC) and Unavailable Check Cancellation (UCC) files from each of the 4 RFCs, the DMC, and those UCCS entered online in POL or TCIS.
* FMS Treasury Check Operations Re-engineering Effort (T-CORE) at Federal Reserve Bank (FRB) Richmond sends check paid transmittals from the two Federal Reserve Bank Check Processing Offices.
* Defense Finance and Accounting Service (DFAS) sends UCC and check issue data for Department of Defense.
*Office of the Special Trustee for American Indians (Disbursing Office Symbol 4844) sends check issue data for checks they have disbursed and paper UCC documents. The format for their issue transmittals has two additional data elements from the standard issue transmittal format; the payee's last name and zip code.
* FMS STAR system sends Agency Location Code (ALC) Master File.
* Treasury Receivable, Accounting and Collection System (TRACS) sends case history information updates on check claims or reclamations.
* Federal Records Center (FRC) sends original negotiated U.S. Treasury checks which are scanned into TCIS.

* Federal Reserve System's Image Service System (ISS) provides digital check images of negotiated U.S. Treasury checks requested to resolve check reconciliation or claims cases.
*Completed Claim Forms from Payees are received at FRB Philadelphia or at FMS in Hyattsville and scanned into the TCIS Document Management System.

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Information may come from the individual claimant, but mostly it is from other sources, as listed above. The information to be stored in the system comes from a number of entities. Check issuance and cancellation information is provided by Treasury Disbursing Offices (TDOs) and NTDOs. Paid check information is received from the FRB. Information from payees may also be stored in the system. Checks and ACH payments are for various types of payments including benefit, salary, vendor, and miscellaneous payments.

b. What Federal agencies are providing data for use in the system?

All FPAs, who are authorized to make benefit, salary, vendor, and miscellaneous payments, originate various types of information that is to be stored in TCIS. For FPAs that use TDOs, this information will come from FMS' RFCs that make payments on their behalf. For FPAs that use their own disbursing officers, information is provided directly from them into TCIS. In addition, some data also will come into TCIS via other FMS systems.

c. What Tribal, State and local agencies are providing data for use in the system?

The Office of the Special Trustee for American Indians (Disbursing Office Symbol 4844) provides TCIS check issue data for checks they have disbursed and paper UCC documents. Issues transmittals generally include the issue transmittal number, accounting date, check symbol number, check serial number, issue date, issue amount, payee ID, ALC, appropriation code (Treasury Account Symbol) and the item count and dollar amount of all the individual records contained in the transmittal. The format for issue transmittals received from the Office of the Special Trustee for American Indians has two additional data elements from the standard issue transmittal format; the payee's last name and zip code.

d. From what other third party sources is the data collected?

Information on paid checks and check images (when needed) will also be provided to TCIS by the Federal Reserve System. ACH payment information will come from PACER.

e. What information will be collected from the employee and the public?

Payment information from the public may include transaction amounts, methods of payment, financial accounts information, names, addresses, taxpayer identification numbers, agencies authorizing the payment, Treasury and agency account symbols, transaction identifiers, transaction dates, and transaction statuses. Various administrative information is also associated with the system, including employee usernames and passwords.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than FMS records be verified for accuracy?

The various files described above will be subject to various forms of automated validations prior to processing to check for accuracy. These validations ensure that information is properly formatted. In addition, it also entails other general types of verification (e.g. ensuring valid agency information). These validation rules are primarily set by FMS.

Information related to the issuance and payment of checks and ACH payments is also subject to validation by FMS in the normal course of reconciling and adjudicating checks and ACH payments. Certain information within the system will be subject to online correction by FMS employees. Field edits are performed to assure necessary information has been entered.

b. How will data be checked for completeness?

The various files described above will be subject to various forms of automated validations prior to processing to check for completeness. These validations ensure that fields deemed mandatory have data within them (e.g., check symbol serial number). These validation rules are primarily set by FMS.

Authentication information provided by end-users is subject to browser-based and server-based error checking to ensure that the information is complete.

Control totals follow NIST guidelines.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

All information provided by FMS TDOs/RFCs, NTDOs, FRS and FMS internal systems and end users goes through their control checks first.

TCIS performs edits on dates and duplicates when validating data it receives. Files are edited against future dates or past dates based on criteria set in the system.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data elements are essentially delineated in the IV, Frontier, Solver, and TCDOMS user guide glossaries as well as the application help screens.

C. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes. All information collected and disseminated is relevant and necessary for FMS to fulfill its lawful mission. FMS is responsible for reconcilement of all U.S. Treasury checks disbursed world-wide and the adjudication of all claims made on U.S. Treasury checks.

System profile data is needed to ensure compliance with government security laws and regulations.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

3) Will the new data be placed in the individual's record?

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

4) Can the system make determinations about employees/public that would not be possible without the new data?

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

5) How will the new data be verified for relevance and accuracy?

N/A. The system will not derive new data or create previously unavailable data about an individual through aggregation from the information collected.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

Data will be retained in the system primarily for reconciliation and check claims purposes. Data may be consolidated for reporting purposes related to check reconcilement and check claims functions. This may include management information data.

Data related to the administrative management of the system may also be consolidated. Such information may be made available to database administrators and program representatives, including developers, as determined by the TCIS system owner as needed to investigate improvements, security breaches, or possible error resolution.

All access to any consolidated data is subject to the same restraints as set out above for non-consolidated data.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

All access to any consolidated data is subject to the same restraints as set out above for non-consolidated data. Users are restricted to view only data that they have been authorized to access through user provisioning and TCIS access controls (e.g., access given by ALCs and read or read/write access).

8) How is the data to be retrieved? Can it be retrieved by personal identifier? If yes, explain. How are the effects to be mitigated?

Data from the system is generally retrieved by check symbol/serial number, a non-personal identifier. TCIS Integrated View (IV) only allows for the query of information by payee ID (within a date range), ACH # or check symbol/ serial number. You cannot query by name or address. However, the social security number is commonly used as the payee ID field. This is mitigated by the fact that those agencies accessing the system can only see their own data.

Database administrators will be able to retrieve data from databases and system administrators from audit logs by personal identifier. There are checks

in place for powerful users relating to audit logs, recertification, access to least privileged and other security controls.

The effects are mitigated as described above.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

The system is not designed to produce reports on individuals. Division management can get case workload statistical information.

D. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

TCIS will be operated from more than one site. TCIS will be operated from Dallas, TX. The Integrated View module will be operated from Hyattsville, MD. IV is a query function of the system to access and display information contained in CP&R, PACER on-line, and TCIS.

2) What are the retention periods of data in this system?

TCIS will follow appropriate data retention planning, NARA and legal requirements when applicable. The normal retention period for the data in the system is seven years. However, FMS is currently retaining all data in this system indefinitely, due to pending litigation.

TCIS will follow retention schedule N1-425-01-4. This is a pending schedule which allows for the transfer of paper records to a Federal Records Center; it cannot be used to destroy/delete records until NARA approves the schedule. NARA will not approve the schedule (N1-425-01-4), until litigation issues involving the records are resolved.

From (N1-425-01-4), item 1
A. Inputs: Delete input files 30 days after input and verification
B. Master File— (1) Individual Indian Monies (IIM) records: Delete from database and index when 20 years old
(2) Non-IIM (all other) records: Delete from database and index when 7 years old
C. Outputs— (1) Output files to other systems: Delete 30 days after output
(2) Electronic versions of output reports: Delete from data base when 20 years old

(3) Paper versions of output reports: Destroy when no longer needed for agency business

D. Documentation: Maintain for life of system plus 3 years

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

Due to pending litigation, FMS is not eliminating any data from this system and does not plan to do so in the foreseeable future. (The only exception is digital check images requested to resolve check reconciliation cases which are retained for sixty (60) days. FRS maintains all images indefinitely and any image may be requested if it is subsequently needed. Other digital check images and original physical checks are currently retained indefinitely.)

4) Is the system using technologies in ways that the FMS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

The new system will use PKI level II authentication for all Internet users.

5) How does the use of this technology affect public/employee privacy?

The use of this technology allows for more efficient retrieval and processing of data needed in the routine course of business. Some of this data may be personal in nature. However, procedures surrounding its care and use as described earlier will not change.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The information in the system is static information related to the issuance of check payments to payees. Certain personal information may be available related to their issuance (e.g., name and address) and may be used in various check after-math processes. The system does not identify or monitor individuals.

For security purposes, to safeguard information contained in the system, software will be employed to monitor access to the system. A log will kept of valid and invalid attempts to gain access to the system; it may include date, user id, password, and log-on/log-off-related information. Audit log information has limited access. TCIS will comply with FMS standards.

For administrative purposes, the system will also retain information related to the identity of employees that have made changes or completed processes within the system in the normal course of business.

The use of cookies will be minimized and, when actually used, the session cookies will be stored in RAM and will not be written to the user's computer.

7) What kinds of information are collected as a function of the monitoring of individuals?

TCIS does not monitor individuals.

8) What controls will be used to prevent unauthorized monitoring?

The system will not actively monitor individuals or groups.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Pursuant to the Privacy Act of 1974, as amended, 5 U.S.C. 552a, FMS has established the following applicable system of record number and titles.

Payment Issue Records for Regular Recurring Benefit Payments—Treasury/FMS .002
Payment Records for Other Than Regular Recurring Benefit Payments—Treasury/FMS .016

Claims and Inquiry Records on Treasury Check and International Claimants—Treasury/FMS .003

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

TCIS will eventually replace CP&R. However, the basic information used in both the new and old systems will not change. Therefore, an amended System of Records (SOR) is not required.

E. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Information in the system is generally available to FMS employees according to the authorities granted to them. Employees are counseled that they may only view information available to them on a "need-to-know" basis in the performance of their duties. Personnel associated with other federal agencies also have access to information for their particular agency. The information of one agency may not be viewed by another agency. In addition, data will be

available to various FMS and FRB personnel and any of their contractors in the performance of their normal duties.

2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

Information that is collected and used with respect to payees is necessary and relevant to the check after-math processes or other legally mandated or authorized purposes. The information within the system that will be available to various parties in the normal course of business is approved by the director-level system owner of record, his/her acting manager designee, or higher senior executive. FMS receives much of the information related to this system from program agencies, but also receives it from other sources as well in the course of carrying out its mission related to check after-math processes. These sources include Federal Reserve banks and payees.

Procedures will be in place for the new system that are similar to those in place for the current system. FMS will be primarily responsible for administration of FMS users. Federal agency administrators will be primarily responsible for ensuring compliance of security procedures within their respective agencies. Documentation will detail who may have what level of access in the system. All access requests must be placed in writing within a formal access control system. All requests will be approved by appropriate personnel prior to granting access. The system will keep detailed logs of actions taken by each employee. The Treasury Web Applications Infrastructure (TWAI) as well as designated FMS employees will monitor access, investigate potential security violations, and take appropriate remedial action if needed.

Interfacing files with the system come and leave the system via secure means for sensitive but unclassified data. For the new system, if possible, it is envisioned that there will be one communications protocol with the TCIS system. The security requirements for the interfacing files will be no different than what is in practice for the current system. There is no change in the level of security for these interfacing files.

All FMS employees as well as Federal Reserve Bank (FRB) employees undergo a background investigation prior to employment. All contractor employees must also undergo a background investigation if they will be working on the TCIS application. All FMS personnel sign a “Rules of Behavior” statement that delineates requirements for system use.

Access to data by an end-user requires that an end-user be authenticated using a TCIS username and password. In addition, two-factor authentication is provided by a PKI or a user gaining access from a trusted site at an agency over a T-1 line.

In addition to those referenced, the above is part of various business and security requirements, standard operating procedures, and in agreements. These requirements and others are delineated in several documents, including the Privacy Act of 1974, as amended, the FMS Security Manual (last updated 4/21/05), the FMS Privacy Act Overview policy (last updated10/7/04), the FMS Sensitive Information Security Controls policy (last updated 7/29/04), and the FMS Sensitive Information Control standard (last updated 7/29/04).

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

FMS users will have access to that data and those actions needed in the normal performance of their duties. Certain actions will be limited to appropriate supervisors in FMS.

Agency personnel will have access to data only for their own agency or have access to a subset of the data for their agency. Agency personnel will primarily have inquiry access, but may be able to make certain requests for FMS action online—as is the case with the current system.

TCIS database administrators will have access to database information. Program managers at FMS, FRB, and TWAI as well as system administrators (including the FMS application information system security officer, FRB personnel, and TWAI personnel) will have access to audit logs of actions taken within the system. This is required for monitoring unauthorized access and/or use of the system.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?**

All FMS personnel must attend mandatory annual security training. This training includes a review of selected security procedures. All personnel associated with the TCIS system must sign a "Rules of Behavior" document. Those agreeing to the Rules of Behavior signify that they understand the IT security requirements, accept the IT security requirements, and acknowledge that disciplinary action may be taken based on violation of the Rules of Behavior. It applies to all FMS employees, contractors, fiscal agents, financial agents, and subcontractor personnel who access IT systems and the facilities where FMS information is processed, transmitted, and stored as well as to all physical space housing IT systems, communications equipment, and supporting environmental control infrastructure that impact IT areas.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were

Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Yes.

6) Do other systems share data or have access to the data in the system? If yes, explain.

As previously noted, TCIS receives information from external entities. These external entities are responsible for protecting privacy rights of information residing with them. Similarly, information that is provided to other systems have responsibility of protecting privacy rights related to the information such systems receive.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

TCIS system owner.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

Personnel associated with other federal agencies also have access to information for their particular agency. The information of one agency (or subset thereof) may not be viewed by another agency (or subset thereof).

Procedures will be in place for the new system that are similar to those in place for the current system. FMS will be primarily responsible for administration of FMS users. Federal agency administrators will be primarily responsible for ensuring compliance of security procedures within their respective agencies. Profile information will be created by federal agency authentication administrators. Documentation will detail who may have what level of access in the system. All access requests must be placed in writing within a formal access control system. All requests will be approved by appropriate personnel prior to granting access. The TWAI as well as designated FMS employees will monitor access, investigate potential security violations, and take appropriate remedial action if needed.

Access to data by an end-user requires that an end-user be authenticated using a TCIS username and password. There are two authorities for system security—one is from a platform perspective and the other is from an application perspective. Security procedures are well documented by the TWAI.

It should be noted that much of the information within the system is often that which was originated by the federal agencies and is resident in their systems. Data will normally only be disclosed to those agencies that originated payments that led to reconcilement and adjudication information. Any other disclosures will be made only in accordance with the provisions of 26 USC 6103 (restricting the disclosure of tax return information), 5 USC 552a (the Privacy Act) and 18 USC 1905 (the Trade Secrets Act), and other applicable laws and will be made using the procedures outlined above.

The TCIS system owner will have responsibility for ensuring compliance.

9) How will the data be used by the other agency?

As mentioned above, much of the information within the system is often that which was originated by the federal agencies and is resident in their systems. Data will normally only be disclosed to those agencies that originated payments that led to reconcilement and adjudication information.

10) Who is responsible for assuring proper use of the data?

The system owner.